

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-328090

(P2004-328090A)

(43) 公開日 平成16年11月18日(2004.11.18)

(51) Int. Cl.⁷

F I

テーマコード (参考)

H04L 9/08

H04L 9/00 601B

5B017

G06F 12/14

G06F 12/14 310Z

5C063

G06F 13/00

G06F 13/00 540R

5C064

G06F 17/60

G06F 17/60 142

5J104

H04N 7/08

G06F 17/60 302E

審査請求 未請求 請求項の数 9 O L (全 14 頁) 最終頁に続く

(21) 出願番号 特願2003-116450 (P2003-116450)
(22) 出願日 平成15年4月22日 (2003.4.22)(71) 出願人 000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目6番地
(74) 代理人 100075096
弁理士 作田 康夫
(72) 発明者 宮本 啓生
神奈川県川崎市麻生区王禅寺1099番地
株式会社日立製作所システム開発研究所
内
(72) 発明者 鶴飼 ひろみ
神奈川県川崎市麻生区王禅寺1099番地
株式会社日立製作所システム開発研究所
内
Fターム(参考) 5B017 AA02 BA07 CA16
5C063 AB05 AC01 CA23 DA07 DB09
最終頁に続く

(54) 【発明の名称】 コンテンツ配信システム

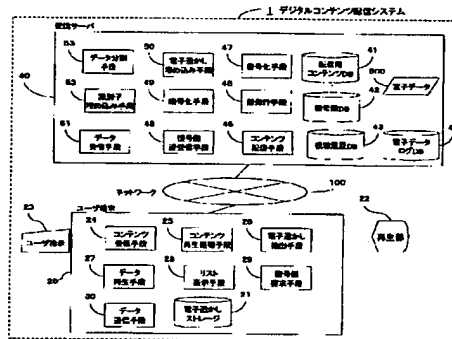
(57) 【要約】

【課題】 コンテンツに埋め込まれた電子データに対する不正を抑制して、コンテンツの視聴率を正確に把握する。

【解決手段】 配信サーバ40が、電子データを暗号化する暗号化手段49と、暗号化電子データを電子透かしを用いてコンテンツに埋め込む埋め込み手段50と、暗号化電子データを復号するための復号鍵を管理する鍵発行手段46及び復号鍵DB42と、コンテンツをユーザ端末に配信する配信手段45を有し、ユーザ端末20が、コンテンツをダウンロードする受信手段24と、コンテンツを再生する再生処理手段25と、コンテンツを再生した場合に電子透かし情報を抽出する抽出手段26と、電子透かし情報を配信サーバへ送信する送信手段30を有し、配信サーバが、電子透かし情報をユーザ端末から受信した場合に暗号化電子データに応じた復号鍵をユーザ端末へ送信する送信手段48を有する。

【選択図】 図1

【図1】



【特許請求の範囲】

【請求項1】

配信サーバからユーザ端末へデジタルコンテンツを配信するためのコンテンツ配信システムにおいて、

前記配信サーバは、電子データを暗号化する暗号化手段と、暗号化電子データを電子透かしを用いてデジタルコンテンツに埋め込む埋込手段と、前記暗号化電子データを復号するための復号鍵を管理する管理手段と、前記暗号化電子データが埋め込まれたデジタルコンテンツをユーザ端末に配信する配信手段を有し、

前記ユーザ端末は、前記デジタルコンテンツを前記配信サーバからダウンロードするダウンロード手段と、前記デジタルコンテンツを蓄積する蓄積手段と、前記デジタルコンテンツを再生する再生手段と、前記再生手段が前記デジタルコンテンツを再生した場合に前記デジタルコンテンツに埋め込まれている前記暗号化電子データを含む電子透かし情報を抽出する抽出手段と、前記電子透かし情報を前記配信サーバへ送信する送信手段を有し、
前記配信サーバは、さらに、前記電子透かし情報を前記ユーザ端末から受信した場合に、前記電子透かし情報に応じた電子データ又は前記電子透かし情報に含まれる暗号化電子データを復号するための復号鍵を前記ユーザ端末へ送信する送信手段とを有することを特徴としたコンテンツ配信システム。

【請求項2】

デジタルコンテンツを配信するためのコンテンツ配信装置において、

電子データを暗号化する暗号化手段と、

暗号化電子データを電子透かしを用いてデジタルコンテンツに埋め込む埋込手段と、

前記暗号化電子データが埋め込まれたデジタルコンテンツをコンテンツ再生装置へ配信する配信手段と、

前記コンテンツ再生装置が前記デジタルコンテンツを再生した場合に、前記デジタルコンテンツに埋め込まれた電子透かし情報及び前記電子データの要求を前記コンテンツ再生装置から受信する受信手段と、

前記電子透かし情報及び前記電子データの要求を前記コンテンツ再生装置から受信した場合に、前記電子透かし情報に応じた電子データを前記コンテンツ再生装置へ送信する送信手段を備えたことを特徴としたコンテンツ配信装置。

【請求項3】

前記電子透かし情報から前記暗号化電子データを抽出する抽出手段と、

前記暗号化電子データを復号するための復号鍵を蓄積する蓄積手段と、

前記暗号化電子データを復号するための復号鍵を前記蓄積手段から検索する検索手段と、

検索された前記復号鍵を用いて前記暗号化電子データを復号する復号手段を備え、

前記送信手段は、復号して得た前記電子データを前記コンテンツ再生装置へ送信することを特徴とした請求項2のコンテンツ配信装置。

【請求項4】

前記電子データごとに前記コンテンツ再生装置へ送信した電子データの数をカウントする計測手段を備え、

前記送信手段は、前記コンテンツ再生装置へ送信した電子データの数が予め定められた数を超過した場合に、前記コンテンツ再生装置への前記電子データの送信を中止することを特徴とした請求項2のコンテンツ配信装置。

【請求項5】

前記電子透かし情報及び前記電子データの要求を前記コンテンツ再生装置から受信した場合に、前記電子透かし情報に基づいて前記デジタルコンテンツを特定し、前記デジタルコンテンツの視聴履歴として管理する視聴履歴管理手段を備えたことを特徴とした請求項2のコンテンツ配信装置。

【請求項6】

前記暗号化電子データをn個のデータ片に分割し、元が同じ暗号化電子データであることを示すグループ識別子と各データ片に対しシリアルに付与されたシリアル識別子を各デー

10

20

30

40

50

タ片に付与する分割手段を備え、

前記埋込手段は、前記グループ識別子と前記シリアル識別子を含む各データ片を電子透かしを用いて複数のデジタルコンテンツの各々に埋め込むことを特徴とした請求項2のコンテンツ配信装置。

【請求項7】

前記n個のデータ片のうち、m番目のシリアル番号のデータ片は、(m+1)番目のシリアル番号のデータ片の復号鍵であることを特徴とした請求項6のコンテンツ配信装置。

【請求項8】

デジタルコンテンツを配信するためのコンテンツ配信装置において、

電子データを暗号化する暗号化手段と、

暗号化電子データを電子透かしを用いてデジタルコンテンツに埋め込む埋込手段と、

前記暗号化電子データを復号するための復号鍵を蓄積する蓄積手段と、

前記暗号化電子データが埋め込まれたデジタルコンテンツをコンテンツ再生装置へ配信する配信手段と、

前記コンテンツ再生装置が前記デジタルコンテンツを再生した場合に、前記デジタルコンテンツに埋め込まれた電子透かし情報及び前記復号鍵の要求を前記コンテンツ再生装置から受信する受信手段と、

前記電子透かし情報及び前記復号鍵の要求を前記コンテンツ再生装置から受信した場合に、前記電子透かし情報に基づいて前記復号鍵を前記蓄積手段から検索する検索手段と、

前記復号鍵を前記コンテンツ再生装置へ送信する送信手段を備えたことを特徴としたコンテンツ配信装置。

【請求項9】

前記復号鍵ごとに前記コンテンツ再生装置へ送信した復号鍵の数をカウントする計測手段を備え、

前記送信手段は、前記コンテンツ再生装置へ送信した復号鍵の数が予め定められた数を超過した場合に、前記コンテンツ再生装置への前記復号鍵の送信を中止することを特徴とした請求項8のコンテンツ配信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、電子透かしを用いて電子データをデジタルコンテンツに埋め込み、そのデジタルコンテンツを配信するための方法およびシステムに関する。

【0002】

【従来の技術】

電子透かしは、オリジナルコンテンツにコンテンツのID等のデータを可視または不可視のデータとして埋め込む技術であり、オリジナルコンテンツを改ざんしても透かしデータが消えないという特徴を利用して、著作権情報を透かしで埋め込むことでコンテンツの不正利用を検知し、著作権を保護する目的で使われている。また、コンテンツを再生することによって埋め込まれた電子透かしを抽出することができるという特徴を持っている。以上のことを利用した従来技術として、例えば、著作権情報、購入者情報、利用者情報、利用制限情報、極秘情報を電子透かしとしてデジタルコンテンツに付加し、デジタルコンテンツの不正利用を防止する技術が開示されている（非特許文献1参照）。

【0003】

一方、端末でのデジタルコンテンツの視聴を配信サーバ側で確認する従来技術として、デジタルコンテンツを複数に分割し、分割した部分のコンテンツを視聴する度にアンケートを行い、視聴履歴を取得する技術が開示されている（特許文献1参照）。

【0004】

【非特許文献1】松井甲子雄著「電子透かしの基礎」森北出版株式会社、1998年8月21日、(ISBN 4-627-82551-X) p. 9-12、p. 132-194

【特許文献1】特開2002-359834号公報

【0005】

【発明が解決しようとする課題】

上記非特許文献1の従来技術では、電子透かしの一般的な用途である利用条件や配信先情報を透かしとしてデジタルコンテンツに埋め込む方法を利用して、利用条件に違反した二次利用や不正な再配布を防止する技術が開示されている。しかし、それらは様々なデジタルコンテンツの不正利用を検出する技術が主であり、抽出後の透かしデータが不正に利用されてしまう恐れがある。

【0006】

上記特許文献1の従来技術では、詳細な視聴履歴を取得するために、デジタルコンテンツを前半と後半に分け、デジタルコンテンツの序盤、中盤、終盤のタイミングで視聴者にアンケートを要求し、回答しなければ続きのデジタルコンテンツを視聴できないようになっている。そのため、ユーザがデジタルコンテンツを視聴する際に数度にわたって、リモコン等を操作し、アンケートを回答するという手間を強いられるため、ユーザの負担が大きくなる。

10

【0007】

本発明の目的は、デジタルコンテンツに埋め込まれた電子データに対する不正を抑制できるシステム及び方法を提供することである。

【0008】

本発明の目的は、デジタルコンテンツの視聴者（利用者）の負担を軽減しつつ、デジタルコンテンツの視聴率（利用率）を正確に把握できるシステム及び方法を提供することである。

20

【0009】

【課題を解決するための手段】

第1の観点として、配信サーバにおいて、暗号化した電子データを含む透かしデータを電子透かしでデジタルコンテンツに埋め込み、当該デジタルコンテンツをユーザ端末に配信する手段と、暗号化した電子データの復号鍵を管理する手段を持ち、ユーザ端末はデジタルコンテンツ再生時に電子透かし情報を抽出する手段を持つデジタルコンテンツ配信システムを提供する。電子透かしによって埋め込まれた暗号化した電子データを含む透かしデータは、デジタルコンテンツを再生することによってしか抽出することができないことを利用して、ユーザが透かしデータを取得することで当該デジタルコンテンツを確実に再生したことを定義することができ、かつ、透かしデータを抽出しただけでは、暗号化されているため、電子データの改ざんをすることができない。

30

【0010】

第2の観点として、第1の観点に加えて暗号化した電子データを利用できるデジタルコンテンツ配信システムを提供する。ユーザは取得した暗号化した電子データの復号鍵を配信サーバから取得するか、もしくは、暗号化した電子データを配信サーバに送信することによって利用することができ、配信サーバではユーザ端末で当該暗号化した電子データを埋め込んだデジタルコンテンツをユーザが視聴したこととして、当該デジタルコンテンツの視聴履歴を蓄積することができる。電子データ利用時に視聴履歴を取得するため、ユーザに対してシームレスに視聴履歴の取得を行うことができる。

40

【0011】

第3の観点として、ユーザがデジタルコンテンツを再生することで、透かしデータを取り出してユーザ端末内の蓄積装置に蓄積し、複数のデジタルコンテンツを再生することによって、関連付けられたn個の透かしデータを収集し、n個の透かしデータに含まれるデータを結合して、ひとつの暗号化した電子データを生成する方法を提供する。配信サーバ内において、1つの電子データを暗号化した後、n個に分割し、個々のデータに対して、本デジタルコンテンツ配信システム内でユニークなデータ識別子と、n個に分割された電子データが同一のグループであることを示すグループ識別子と、結合するときに必要なn個の電子データの順番を示す1からnまでの整数を取るシリアル番号等を付加することによって構成されている。電子データ利用時には分割したデータを統合して復号化を行う。第

50

2の観点のデジタルコンテンツ配信システムに適用することで、1度に複数の視聴履歴を取得することができ、第2の観点を好適に実施することができる。

【0012】

第4の観点として、第3の観点を踏まえてグループ識別子を利用した透かしデータの利用方法を提供する。グループ識別子を持つ暗号化した透かしデータがあり、1から $n-1$ までの任意の整数であるシリアル番号 m の透かしデータは、それ自身が持つ暗号化した電子データを復号化することによって得られるシリアル番号 $m+1$ の透かしデータが持つ暗号化した電子データの復号鍵である。シリアル番号 n を持つ透かしデータは、本デジタルコンテンツ配信システムで有効な電子データが暗号化して入っており、 n 個すべての電子透かし情報を収集すると、ユーザは任意のタイミングで、シリアル番号1の暗号化した電子データを復号化する鍵を配信サーバから取得し、当該電子データを復号化することでシリアル番号2の透かしデータにある暗号化した電子データのシリアル番号3用の復号鍵を取り出し、これを連鎖的に実施することによりシリアル番号 n にある本システムで利用可能な電子データを取り出すことができる。第4の観点のデジタルコンテンツ配信システムに適用することで、1度に複数の視聴履歴を取得することができ、第2の観点を好適に実施することができる。

10

【0013】

第5の観点として、配信サーバの機能として、復号鍵取得要求をしてきたユーザに対して、先着の限定人数にのみ復号鍵を送付する、もしくは、ユーザ端末から暗号化した電子データに対して先着の限定人数にのみ、暗号化した電子データを受信する方法を提供する。電子データの利用可能人数を限定することで、ユーザの購入意欲を促進することができる。第3の観点、第4の観点を踏まえることで、よりユーザの購入意欲を促進することができるデジタルコンテンツ配信システムを提供することができる。

20

【0014】

【発明の実施の形態】

本発明の実施の形態について、図面を参照しながら説明する。本実施の形態は、クーポンや電子マネーなどのユーザにとって価値の高い有価情報を暗号化して識別子を付与し、透かしデータとしてデジタルコンテンツに埋め込み、ユーザ端末の要求に応じて当該デジタルコンテンツを配信することを想定している。電子透かし情報はデジタルコンテンツを再生しなければ、抽出することができないため、透かしデータを抽出した後、その情報に含まれる暗号化した電子データを復号するとき、暗号化した電子データを配信サーバに送ると共に暗号化した電子データの復号を配信サーバに要求するか、もしくは、復号鍵を配信サーバに要求することで配信サーバに履歴が残る。その履歴は、ユーザがデジタルコンテンツを視聴したとして配信サーバが認識し、当該デジタルコンテンツの視聴履歴とすることができる。抽出した透かしデータは、抽出した状態でユーザ端末内の蓄積装置に蓄積することで、ユーザが電子データを不正に操作することを防ぐことができる。

30

【0015】

図1は、本発明の第1実施形態にかかるデジタルコンテンツ配信システム1の基本構成を示すブロック図である。このデジタルコンテンツ配信システム1は、ユーザ端末20と配信サーバ40とをネットワーク100で接続したものである。

40

【0016】

ユーザ端末20は、パーソナルコンピュータやセットトップボックスなどのコンピュータ装置であり、透かしデータ600を蓄積する電子透かしストレージ21と、デジタルコンテンツ再生時にデジタルコンテンツを再生する再生部22と、外部からの入力機器によってユーザ端末20を操作するユーザ指示23と、デジタルコンテンツを受信するコンテンツ受信手段24と、デジタルコンテンツを再生するコンテンツ再生処理手段25と、デジタルコンテンツ再生時に当該デジタルコンテンツに埋め込まれている透かしデータ600を抽出し、電子透かしストレージ21に蓄積する電子透かし抽出手段26と、電子透かしストレージ21内の透かしデータ600をユーザが閲覧できるように再生部22を利用してリストを表示するリスト表示手段28と、電子透かしストレージ21からユーザ指示2

50

3における内容から必要な透かしデータ600を取り出し、暗号化した電子データ500の復号鍵を取得する復号鍵要求手段29と、暗号化した電子データ500を復号化するデータ再生手段27と、生成されたクーポンなどを配信サーバ40に送信するデータ送信手段30を含んでいる。

【0017】

配信サーバ40は、例えばワークステーションであり、配信用コンテンツDB41と、発行した復号鍵を蓄積する復号鍵DB42と、視聴履歴を蓄積する視聴履歴DB43と、デジタルコンテンツ配信システム1で利用可能な例えばクーポンである電子データ500と、デジタルコンテンツ配信手段45と、暗号鍵を発行する鍵発行手段46と、復号鍵要求手段29からのデータ識別子501を受信し、データ識別子501をキーとしてユーザ所望の復号鍵を検索し、ユーザ端末に送信する復号鍵送受信手段48と、鍵発行手段46によって発行された暗号鍵を利用し電子データ500を暗号化する暗号化手段49と、暗号化した電子データ500を透かしデータ600としてデジタルコンテンツに埋め込む電子透かし埋め込み手段50と、ユーザ端末20から送信された電子データ500を受信するデータ受信手段51を含み、さらに、暗号化した電子データ500に付加情報を埋め込む識別子埋め込み手段52と、暗号化された電子データ500をn個に分割するデータ分割手段53と、ユーザ端末から送信された電子データを蓄積する電子データログDB44を含む。

10

【0018】

図2は、配信サーバ40で暗号化手段49によって暗号化され、その後、電子透かし埋め込み手段50によって透かしデータ600としてデジタルコンテンツに埋め込まれる電子データ500の構成内容を示す。データ構成内容は、電子データ500を一意に識別することができるデータ識別子501と、電子データ500が属するグループを一意に識別できるグループ識別子610を含んでいる。電子データ500は、例えば、クーポンのようなユーザが本システム内で利用することができるものである。

20

【0019】

図3は、配信サーバで、電子透かし埋め込み手段50によってデジタルコンテンツに埋め込まれる透かしデータ600、あるいは、ユーザ端末20に存在する電子透かしストレージ21に蓄積される透かしデータ600の構成内容を示す。透かしデータ600はデータ識別子501と、透かしデータ600が属するグループを定義するグループ識別データ601と、電子データ500を暗号化した暗号化データ602によって構成されており、そのうちグループ識別データは、電子データ500のデータ識別子501をグループの識別子とするグループ識別子610と、例えば、グループ内の全データ数やn個目のデータであることを示すフラグなどにあげられるグループ内のデータが揃ったことを検知できる結合識別子611と、グループ内ではユニークであるn個の連続した結合するときの順序を示す番号であるシリアル番号612を含む。

30

【0020】

図4は、配信サーバ40で、透かしデータ600をデジタルコンテンツに埋め込む方法を示した流れ図である。ユーザにデジタルコンテンツ配信システム1を提供するために、その前段階の処理としてデジタルコンテンツに実施されるものである。

40

【0021】

ステップ300において、鍵発行手段46によって暗号鍵を生成する。

【0022】

ステップ302において、ステップ301で生成した暗号鍵を利用して電子データ500を暗号化し、鍵情報は復号鍵DB42に登録する。

【0023】

ステップ304において、識別子埋め込み手段52によって、暗号化した電子データ500にデータ識別子501と、グループ識別子610と、結合識別子611を埋め込む。

【0024】

ステップ306において、電子透かし埋め込み手段50にて、配信用コンテンツDB41

50

からデジタルコンテンツを取りだし、ステップ304における生成物を、電子透かしとして埋め込む。

【0025】

ステップ308において、ステップ306にて、電子透かしを埋め込まれたデジタルコンテンツを配信用コンテンツDB41に登録する。

【0026】

図5は、デジタルコンテンツ配信システムの基本的な流れである。ステップ400～ステップ409で利用されるデジタルコンテンツには、事前にステップ300～ステップ308までの処理が行われているものとする。また、デジタルコンテンツは映像、音声などのデータを想定している。

10

【0027】

ステップ400において、ユーザはユーザ端末20をユーザ指示23からコンテンツ受信手段24を操作して、デジタルコンテンツを受信する。

【0028】

ステップ401において、デジタルコンテンツ配信手段45は、ユーザ端末20に存在するコンテンツ受信手段24からの要求によって、デジタルコンテンツを送信する。

【0029】

ステップ402において、コンテンツ再生処理手段25によって、デジタルコンテンツを再生し、電子透かし抽出手段26では、デジタルコンテンツを再生することによって始めて抽出できる透かしデータ600の抽出を行う。抽出されたデータは、電子透かしストレージ21に蓄積される。

20

【0030】

ステップ403において、リスト表示手段28は、再生部22を利用して電子透かしストレージ21に蓄積されている透かしデータ600のリストを表示する。ユーザは、ユーザ指示23を利用してリストの中から所望の透かしデータ600を選択する。

【0031】

ステップ404において、ステップ403にて選択された透かしデータ600のデータ識別子501を復号鍵要求手段29によって復号鍵送受信手段48へ送信し、当該データ識別子501に対応する復号鍵を取得する。

【0032】

ステップ405において、ユーザ端末20から送られてきたデータ識別子501を用いて復号鍵DB42内を検索し、当該データ識別子501に対応した復号鍵を取得する。取得した復号鍵を当該データ識別子501が送信されてきたユーザ端末20に送信する。

30

【0033】

ステップ406において、ライセンス要求手段29は、復号鍵を受信すると、データ再生手段27が当該復号鍵を使い、透かしデータ600の暗号化データ602に対して復号化を行い、電子データ500を再生する。

【0034】

ステップ407において、データ送信手段30が再生された電子データ500を配信サーバ40に送信することによって、ユーザは電子データ500を利用したことになる。電子データ500は、クーポンとしての利用を想定しているため、例えば、クーポンを送信したユーザに、次のデジタルコンテンツの購入時に支払われる代金の一部、もしくは全てに代わるものを受けることができる。

40

【0035】

ステップ408において、データ受信手段51は、ユーザ端末20から送信されてきたデータ識別子501の受信履歴を、視聴履歴DB43に登録する。視聴履歴は一定期間後、デジタルコンテンツ毎に集計を行い、視聴率を算出するのに用いられる。つまり、どの暗号化データをどのデジタルコンテンツに埋め込んだかを特定するために、暗号化データをデジタルコンテンツに埋め込む際にデータ識別子501とデジタルコンテンツの識別子のテーブルを作成するのが好ましい。そして、テーブルを参照して視聴率を集計したデジタ

50

ルコンテンツに埋め込まれたデータ識別子501を抽出し、データ識別子501の受信数を視聴履歴DB43から算出するのが好ましい。視聴率の算出処理は、配信サーバが実行してもよいし、配信サーバ40は視聴履歴を他の機器へ送信し、その後他の機器が実行してよい。デジタルコンテンツが再生されなければ、電子透かしは情報取り出されないことから、視聴履歴DB43に蓄積されたデータは、デジタルコンテンツの視聴したことを示す視聴履歴データであることが言え、その視聴履歴データを基にして得られるデジタルコンテンツ毎の視聴率は信頼性の高いデータであると言える。

【0036】

ステップ409において、データ送信手段30から送信されてきた電子データ500は、データ受信手段51で受信し、ユーザ毎に電子データ500の受信履歴を電子データログDB44に登録し、ユーザが次回デジタルコンテンツを購入するときに、電子データログDB44を参照して、購入代金の割引などを行う。

【0037】

本システムを利用したサービスにおいて、会員管理を行っていない場合、デジタルコンテンツ毎に得られる視聴履歴は、当該デジタルコンテンツを視聴した全人数をカウントすることが可能であり、当該デジタルコンテンツにおいて視聴率を取得することができる。また、会員管理を行った場合、デジタルコンテンツを視聴した会員の属性情報（性別、年齢、住所等）を利用することにより、当該デジタルコンテンツを好む性別や年齢層などのユーザ属性を調査することができ、当該デジタルコンテンツに連携させた広告を行う場合の指標にすることができる。

【0038】

また、ステップ406以降に関して、暗号化された電子データ500を復号化せずに、暗号化した電子データ500をそのまま、配信サーバ40に送信することも可能である。その場合、配信サーバ40では、送られてきた暗号化された電子データ500を復号化することによって、当該電子データ500の正当性を判断する。当該電子データ500が正当なものであると確認ができると、視聴履歴DB43に当該デジタルコンテンツに視聴があったことを登録する。

【0039】

次に、第2の実施の形態を説明する。第1の実施の形態と同様、電子データ500の利用形態としたクーポンを想定している。ただし、単一の電子データ500が1つのクーポンになるのではなく、複数の電子データ500を集めることによって、1つのクーポンとしての機能を提供できるようにする。ユーザには、電子データ500を収集することによってクーポンを提供するというインセンティブを与えることによって、ユーザのデジタルコンテンツの購入意欲を促進することができる。基本的な電子データを配信して、視聴履歴を取得するシステムは、第1の実施の形態におけるデジタルコンテンツ配信システムと同様である。

【0040】

図6は、上記実施の形態の配信サーバ40におけるデータ500の生成方法を示す流れ図である。図の流れはステップ320～ステップ325で示す。本発明に係わる範囲は、ステップ322～ステップ325である。

【0041】

ステップ320において、鍵発行手段46は、電子データ500を暗号化するための暗号鍵を生成する。

【0042】

ステップ321において、暗号化手段49は、ステップ320で生成した暗号鍵を用いて、電子データ500を暗号化する。

【0043】

ステップ322において、データ分割手段53は、暗号化データ602を任意のn個に分割する。分割には、暗号化データ602のサイズに対してn個へ等分に分割する方法、n個の任意のサイズに分割する方法などがあるが、本発明では特定しない。

【0044】

ステップ323において、識別子埋め込み手段52は、グループ識別子610に電子データ500のデータ識別子501を埋め込み、n個のデータ識別子501を発行し、n個に分割した暗号化データ602各々にデータ識別子501と結合識別子611と、シリアル番号612を埋め込む。

【0045】

ステップ324において、ステップ320で生成した暗号鍵を復号鍵DB42に登録する。

【0046】

ステップ325において、電子透かし埋め込み手段50は、ステップ323で生成したn 10
個の透かしデータをデジタルコンテンツに埋め込み、埋め込んだデジタルコンテンツ配信
コンテンツDB41に登録する。

【0047】

次にユーザ端末20におけるグループ識別子610を利用した電子データ500の利用方法を示す。

【0048】

図7はグループ識別子610を利用した電子データ500の利用方法を示した流れ図である。ユーザは事前に複数のデジタルコンテンツを視聴しており、電子透かしストレージ21 20
内には、いくつかの透かしデータ600が蓄積されているものとする。ステップ430
～ステップ434によってその流れを示す。本発明に係わる範囲は、ステップ430～ス
テップ432である。

【0049】

ステップ430において、リスト表示手段28は、電子透かしストレージ21に存在する透かしデータ600のうち、グループ識別子610が設定されている透かしデータ600を検知すると、同グループ識別子610を持つ透かしデータ600を検索する。

【0050】

ステップ431において、リスト表示手段28は検索を行い結合識別子611を利用して、同グループ識別子610を持つ透かしデータ600の数が足りなかった場合、再生部22 30
を利用してユーザに同グループ識別子610を持つ透かしデータ600が不足していることを表示する。全て揃っている場合には、再生部22を利用してユーザに同グループ識別子610を持つ透かしデータ600がそろったことを通知する。

【0051】

ステップ432において、再生部22に表示された結果に、同グループ識別子610を持つ透かしデータ600がそろったならば、ユーザ指示23に従って配信サーバ40にグループ識別子610を送信し、暗号化した電子データを復号化する鍵のデータ識別子501にユーザ端末20から送信したグループ識別子610に対応した復号鍵を取得する。

【0052】

ステップ433において、データ再生手段27は、同グループ識別子610を持つ透かしデータ600をシリアル番号612順に並べて結合し、取得した復号鍵を利用して、結合した電子データ500を復号化する。 40

【0053】

ステップ434において、データ送信手段30は、ステップ433で再生した電子データ500をデータ受信手段51へ送信する。データ受信手段51は、受信した電子データ500をユーザ毎に電子データログDB44に登録し、ユーザが次回デジタルコンテンツを受信するときに、電子データログDB53を参照して、購入代金の割引などを行う。

【0054】

ステップ433以降において分割データを統合して復号鍵を要求する方法以外に、配信サーバ内で分割データを管理する方法もある。ユーザ端末は分割データ取得した時点でデータ受信手段51に送信し、電子データログDB44に蓄積する。配信サーバ40は、分割データを受信するごとに、すべての分割データが揃ったか否かを判定し、すべて分割デー 50

タがそろったときにユーザ端末20にクーポンが利用できることを通知する。また、分割データが全てそろうまでユーザ端末に蓄積し、全てそろった時点で分割データのまま配信サーバに送信・統合し復号化することで、分割データの正当性を確認しユーザ端末にクーポンが利用できることを通知する方法も可能である。

【0055】

第2の実施の形態を利用し、1連のデジタルコンテンツ（映像や音声）に所定のタイミングでn個の分割したデータを埋め込むことで、当該デジタルコンテンツをユーザが全て再生したことを確認することができる。ユーザ端末で当該デジタルコンテンツを再生し、全て見終わるとn個の分割したデータが、電子透かしストレージ21に蓄積され、復号鍵取得のフェーズに移ることができる。当該デジタルコンテンツの再生を中断してしまうと、
中断した以降のタイミングに埋め込まれている分割データは全て取り出せないため、n個
全てそろうことができず、透かしデータ600を利用するための復号鍵取得のフェーズに
移ることができない。このように、デジタルコンテンツの再生を必ず確認したい場合、例
えば、商品の広告を編集したデジタルコンテンツ等に上記分割データを埋め込むことで、
配信サーバでは、ユーザが確実に広告を再生したことを示す視聴履歴を集めることができ
、商品の広告効果を図る技術として利用できる。ユーザが、デジタルコンテンツをスキッ
プして視聴することも抑制できる。

【0056】

次に、第3の実施の形態を説明する。第1の実施の形態におけるデジタルコンテンツ配信システムを利用することを前提とし、電子データ500の利用の形態としてクーポンを想定
している。ただし、配信サーバ40において、復号鍵を要求してきたユーザの中で先着m
名に対してのみ復号鍵を送信してクーポンの利用を制限する。このときmは任意の正の整
数であり、復号鍵要求を受け付ける最大数である最大受信件数である。復号鍵を取得す
るためにデータ識別子501をユーザ端末から送信するところを、暗号化データ602を送
信することによっても実施できるものとする。これによって、ユーザのデジタルコンテン
ツにおける購入意欲を促進することができる。

【0057】

上記実施の形態は図8にある配信サーバ40におけるライセンス送信手段48の処理手順
によって示す。流れはステップ440～ステップ444で示す。本発明に係わる範囲は、
ステップ441～ステップ444である。なお、復号鍵送受信手段48以外の処理は、第
1の実施の形態と同様である。

【0058】

ステップ440において、復号鍵送受信手段48は、復号鍵要求手段29から送信されて
くるデータ識別子501、あるいは、グループ識別子610を受信する。

【0059】

ステップ441において、復号鍵送受信手段48は、データ識別子501、あるいは、グ
ループ識別子610毎に復号鍵要求の受信件数をカウントする機能と事前に設定した最大
受信件数をカウントした受信件数を比較する機能を持っている。ユーザ端末20からの要
求があるごとに、要求のあったデータ識別子501、あるいは、グループ識別子610の
要求受信件数と最大受信件数を比較し、受信件数に1を足した値が最大受信件数より小
さい、もしくは等しい場合には受信件数に1を足して、ステップ442に遷移する。受信件
数に1を足した値が最大受信件数より大きい場合、最大受信件数を超えたことをデータ送
信手段30に通知する。

【0060】

ステップ442において、ユーザ端末20から送信されてきたデータ識別子501、ある
いは、グループ識別子610の受信履歴を視聴履歴DB43に登録する。

【0061】

ステップ443において、復号鍵送受信手段48は、ユーザ端末20に対して、要求した
データ識別子501、あるいは、グループ識別子610の復号鍵を送信する。

【0062】

第3の実施の形態によりユーザのデジタルコンテンツの購入意欲を促進することができる。

【0063】

次に第4の実施の形態を説明する。第2の実施形態の利用を前提とした複数の透かしデータ600を集めて、1つのクーポンを生成する機能を提供するものである。

【0064】

図10は、第4の実施の形態における透かしデータ600の構造と関連性を示す。ただし、実際に利用できるクーポンはシリアル番号612の n を持つ透かしデータ600だけであり、シリアル番号612の $n-1$ までの透かしデータ600は、全て暗号化した復号鍵が暗号化データ602に入っている。シリアル番号612の m の透かしデータ600が持つ復号鍵は、シリアル番号612の $(m+1)$ の暗号化データ602を復号化する復号鍵であり、シリアル番号612の最も小さい透かしデータ600は、自らの暗号化データを復号する復号鍵を、復号鍵要求手段29を利用して、配信サーバから取得する。ここで言う m は、1から n までの整数である。

【0065】

以上の実施の形態を利用して第5の実施の形態に適用することにより、データ分割手段53に依存することがなくなる。

【0066】

本発明のデジタルコンテンツ配信システムによれば、電子透かしによって埋め込まれた暗号化した電子データは、デジタルコンテンツを再生することによって始めて取り出せることを利用して、ユーザがデジタルコンテンツを再生することによって蓄積した透かしデータ内の電子データを利用するときに、配信サーバに復号鍵を取得する、もしくは、暗号化した電子データを送信することで、デジタルコンテンツに対するユーザの視聴履歴として配信サーバに視聴履歴ログを残し、一定期間の後、集計することによって、デジタルコンテンツに対する信頼性の高い視聴率を取得することができ、ユーザに対してシームレスに視聴履歴を取得することができる。

【0067】

本発明の暗号化した電子データを電子透かし情報としてデジタルコンテンツに埋め込むことで、ユーザが電子データを利用したい場合には、必ず配信サーバから復号鍵を取得するか、もしくは、暗号化データを配信サーバに送信するかをしなければならないため、ユーザの電子データの不正利用を検知する手段を提供できる。

【0068】

本発明のグループ識別子をもつ電子データの使用方法によれば、ユーザが n 個の透かしデータを収集することによって、1つの電子データを取得することで、ユーザは n 個のデジタルコンテンツを再生する必要があり、ユーザの購入頻度を高めることができる。

【0069】

【発明の効果】

本発明によれば、デジタルコンテンツに埋め込まれた電子データに対する不正を抑制できる。

【0070】

本発明によれば、デジタルコンテンツの視聴者（利用者）の負担を軽減しつつ、デジタルコンテンツの視聴率（利用率）を正確に把握できる。

【図面の簡単な説明】

【図1】本発明におけるデジタルコンテンツ配信システムの基本構成図である。

【図2】電子データの構成図である。

【図3】透かしデータの構成図である。

【図4】デジタルコンテンツにデータを埋め込む方法を説明した流れ図である。

【図5】本発明の第1の実施形態にかかるデジタルコンテンツ配信システムの流れ図である。

【図6】本発明の第2の実施形態にかかる透かし情報の生成方法を説明した流れ図である。

【図 7】本発明の第 2 の実施形態にかかる電子データの利用方法を説明した流れ図である。

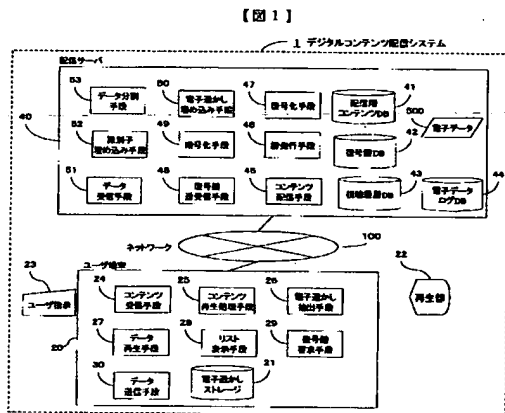
【図 8】本発明の第 3 の実施形態にかかるクーポンの利用者を限定する方法を説明した流れ図である。

【図 9】本発明の第 4 の実施形態にかかる複数の電子データを 1 つのクーポンとして利用する方法を説明した構成図である。

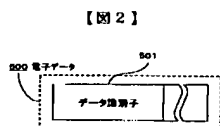
【符号の説明】

1・・・デジタルコンテンツ配信システム、20・・・ユーザ端末、21・・・電子透かしストレージ、22・・・再生部、23・・・ユーザ指示、24・・・コンテンツ受信手段、25・・・コンテンツ再生処理手段、26・・・電子透かし抽出手段、27・・・データ再生手段、28・・・リスト表示手段、29・・・復号鍵要求手段、30・・・データ送信手段、40・・・配信サーバ、41・・・配信用コンテンツ DB、42・・・復号鍵 DB、43・・・視聴履歴 DB、44・・・電子データログ DB、45・・・デジタルコンテンツ配信手段、46・・・鍵発行手段、47・・・復号化手段、48・・・復号鍵送受信手段、49・・・暗号化手段、50・・・電子透かし埋め込み手段、51・・・データ受信手段、52・・・識別子埋め込み手段、53・・・データ分割手段、100・・・ネットワーク、500・・・電子データ、501・・・データ識別子、600・・・透かしデータ、601・・・グループ識別データ、602・・・暗号化データ、610・・・グループ識別子、611・・・グループ内データ数、612・・・シリアル番号。

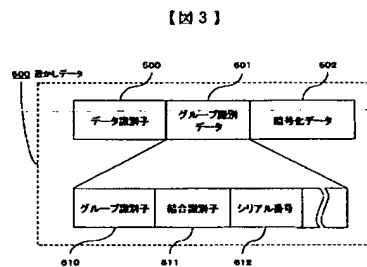
【図 1】



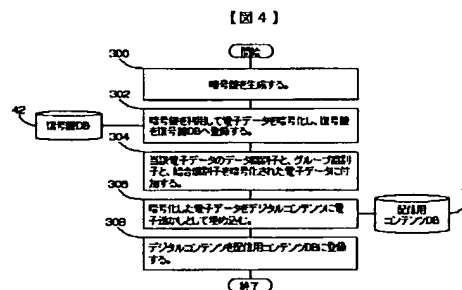
【図 2】



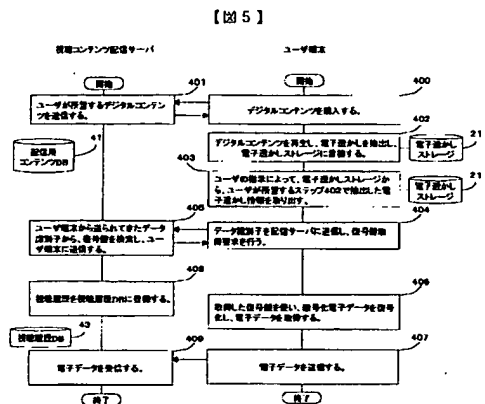
【図 3】



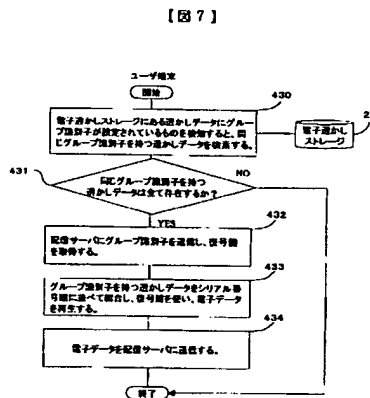
【図 4】



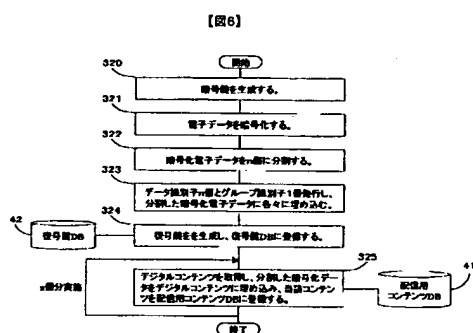
【图 5】



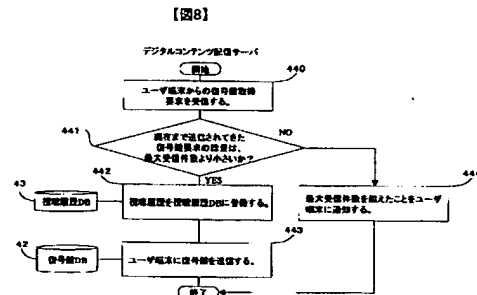
【图 7】



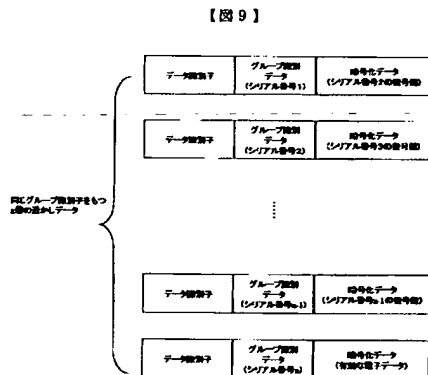
【 図 6 】



【图 8】



【图 9】



フロントページの続き

(51)Int.Cl.⁷

F I

テーマコード (参考)

H 0 4 N 7/081

G 0 6 F 17/60 5 1 2

H 0 4 N 7/173

H 0 4 N 7/173 6 4 0 Z

H 0 4 L 9/00 6 0 1 E

H 0 4 N 7/08 Z E C Z

F ターム(参考) 5C064 BA01 BB10 BC17 BC18 BC22 BC23 BD01 BD02 BD08 BD09
5J104 EA16 PA10